

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of:)
Information associated with Reddit account identified) Case No. 8:23-MJ-00467
as "Sweet-Explanation-81" that is within the)
possession, custody, or control of Reddit Inc.)
)

APPLICATION FOR WARRANT BY TELEPHONE PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A-II

There are now concealed or contained the items described below:

See Attachment B-II

The basis for the search is:

- ☒ Evidence of a crime;
- ☒ Contraband, fruits of crime, or other items illegally possessed;
- ☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)

Offense Description

18 U.S.C. § 2422(b)

enticement of a minor to engage in criminal sexual conduct

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/ Davis Mendelsohn

Applicant's signature

Davis Mendelsohn, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

City and State: Santa Ana, California

Judge's signature

Honorable John D. Early, U.S. Magistrate Judge

Printed name and title

AUSA: Melissa S. Rabbani (x3499)

AFFIDAVIT

I, Davis Mendelsohn, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I have been a special agent (SA) with Homeland Security Investigations (HSI), the investigative component of the United States Department of Homeland Security's Immigration and Customs Enforcement (ICE), since January 2019. I am currently assigned to HSI's Office of the Resident Agent in Charge in Monterey, California. As part of my daily duties, I investigate violations of federal laws related to the sexual exploitation of minors. Prior to my employment with HSI, beginning in June 2016, I was a sworn investigator with the California Department of Motor Vehicles (DMV). While employed with the DMV, I conducted investigations related to a variety of criminal and administrative offenses.

2. Throughout my law enforcement career, I have received training on conducting criminal investigations, search and seizure laws, and writing probable cause affidavits. In 2017, I completed a 24-week-long basic police academy in California, and in 2019, I completed the Criminal Investigator Training Program and HSI Special Agent Training program, a total of 26 weeks of training, at the Federal Law Enforcement Training Center in Brunswick, Georgia. Since becoming a federal law enforcement officer, I have written probable cause affidavits in support of multiple federal search warrants and complaints for cases involving the sexual exploitation of children. I also have a

bachelor's degree in justice studies with a minor in forensic studies from San Jose State University.

3. I make this affidavit in support of an application for search warrants for:

a. As described further in Attachment A-I, the person of Gilmar ABARCA, ABARCA's Honda Civic, and ABARCA's residence, 7284 Chippewa Circle in Buena Park, California (the "SUBJECT RESIDENCE") (collectively, the "SUBJECT LOCATIONS").

b. As described further in Attachment A-II, information associated with a Reddit account - identified as "Sweet-Explanation-81" (the "SUBJECT ACCOUNT") - that is stored at premises controlled by Reddit Inc. (hereinafter, the "PROVIDER"), a provider of electronic communication and remote computing services headquartered at 548 Market Street, San Francisco, California 94104.¹

4. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A),

¹ Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

2703(c)(1)(A), and 2703(d)² to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B-II. Upon receipt of the information described in Section II of Attachment B-II, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B-II. Attachments A-I, A-II, B-I, and B-II are incorporated herein by reference.

5. As described more fully below, I respectfully submit there is probable cause to believe that the SUBJECT LOCATIONS, and information associated with the SUBJECT ACCOUNT, contain evidence, contraband, fruits, or instrumentalities of attempted criminal violations of 18 U.S.C. § 2422(b), enticement of a minor to engage in criminal sexual conduct (the "SUBJECT OFFENSE").

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

² The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B-II paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B-II paragraph II.10.b.).

information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. DEFINITIONS

7. The following definitions apply to this affidavit its associated attachments:

a. **Chat:** Any kind of text communication over the Internet that is transmitted in real time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. **Child Erotica:** Any materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. **Child Pornography:** As defined in 18 U.S.C. § 2256(8) and referred to as "child sexual abuse material (CSAM)" throughout this affidavit, any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in

sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. **Internet Protocol (IP) Address:** A unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static" if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. **Minor:** Defined in 18 USC § 2256(1) and refers to any person under 18 years of age.

f. **Sexually Explicit Conduct:** Defined in 18 USC § 2256(2)(A) and means actual or simulated sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal), whether between persons of the same or opposite sex, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic areas of any person.

g. **Visual Depictions:** Defined in 18 USC § 2256(5) and includes undeveloped film and videotape, data stored on computer disc or other electronic means which is

capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

III. BACKGROUND ON REDDIT

8. Reddit is an online forum owned and operated by the PROVIDER, a company headquartered in San Francisco, California. Reddit users create and moderate online communities known as "subreddits" or "subs." Each subreddit has its own page with a URL in the format reddit.com/r/sub-reddit-name. Reddit users can post text, video, photos, and links to other websites subject to subreddit rules. Subreddits are moderated by selected users. Reddit users are able to "upvote" and "downvote" content resulting in a cumulative score for content and individual Reddit users known as "karma." According to the Reddit website, Reddit "is home to thousands of communities, endless conversation, and authentic human connection."

9. According to Reddit's law enforcement guide, Reddit collects subscriber information such as subscriber identity, IP logs, email address (if provided), and the user's name (if provided). Reddit also collects user preference data, account settings, and communication headers, the contents of posts, comments, and "other information regarding the substance of a user's publicly available communications." The last category of information is available due to its publicly available nature. Finally, Reddit collects the contents of non-public communications including direct messages, information about a

user's voting, and posts, comments, and other information regarding the substance of a user's communications on non-public subreddits.

IV. SUMMARY OF PROBABLE CAUSE

10. In July 2023, I became involved in an investigation related to the sexual exploitation of a 16-year-old female (V-1).³ During the investigation, I learned multiple adult males had sexually exploited V-1. I obtained consent from V-1's mother to search and take control of various online accounts previously used by V-1.

11. While reviewing messages V-1 exchanged with others through Reddit, I observed two separate conversations between V-1 and a subject ("S-1") using the SUBJECT ACCOUNT. I later determined S-1 was likely Gilmar ABARCA, a 23-year-old male from Buena Park, California, a city within the Central District of California. While acting in an undercover capacity as V-1, I took over both conversations between S-1 and V-1, one of which included discussions about V-1 wanting to run away from home. S-1 stated he would allow V-1 to stay with him if she agreed to have sex with him.

V. STATEMENT OF PROBABLE CAUSE

INITIAL CONSENT OBTAINED FROM V-1's MOTHER

12. On July 13, 2023, United States Magistrate Judge Nathanael Cousins for the Northern District of California signed

³ On September 7, 2023, Magistrate Judge John D. Early signed a criminal complaint (8:23-mj-00457-DUTY) charging ABARCA with one count of the SUBJECT OFFENSE. V-1 in the affidavit supporting the criminal complaint is a different individual than V-1 in this affidavit.

a federal search warrant (CR 23-71037-NC) authorizing the search of multiple electronic devices, including V-1's phone. In reviewing V-1's phone, I observed V-1 used several Reddit accounts to communicate with other Reddit users. Many of the conversations were sexually explicit.

13. On August 4, 2023, V-1's mother provided signed consent allowing me to search and take control of three of V-1's Reddit accounts. I subsequently located messages, described in greater detail below, between the SUBJECT ACCOUNT and two of V-1's Reddit accounts.

REDDIT CHATS BETWEEN SUBJECT ACCOUNT AND VICTIM ACCOUNT 1

14. On May 8, 2023, V-1 used Victim Account 1 to submit two separate public posts on Reddit. V-1 submitted both posts before 2:00 AM. One of the posts was titled, "My hypersexuality is making me want to end it." Neither post listed V-1's age at the time of the posts.

15. On May 8, 2023, at approximately 11:06 AM, V-1's Victim Account 1 received a chat message from S-1, who was using the SUBJECT ACCOUNT, asking, "Hey looks like you could use someone to talk to, want to talk?" V-1 and S-1 then began communicating through Reddit. Early in the conversation, S-1 asked V-1 where she was from and how old she was and stated he was 23 years old and from Orange County in Southern California. V-1 told S-1 she was from Monterey County and that she was 16 years old.⁴

⁴ From government records and my investigation of this matter, I know V-1 was actually 15 years old at this time and that she turned 16 years old in June 2023.

16. S-1 told V-1 he messaged her because he did not want her to kill herself and stated, "I won't do anything sexual to you so I don't trigger your hypersexuality." S-1 then began asking V-1 questions regarding sex and romantic relationships such as whether she was in a relationship, whether she loved the person with whom she was having sex, and when the last time she had sex was.

17. At 1:19 PM, S-1 asked, "Is masturbating not enough or do you need sex?" Then, at approximately 1:21 PM, S-1 and V-1 exchanged the following messages:

S-1: Do you want my help in getting off from sex with older people or do you wanna keep doing that and just want someone to talk with about your life

V-1: I'm not sure cause ik I should stop but I don't think I even can cause I don't have anyone else in my life

V-1: If I didn't have them I'd be completely alone irl
[in real life]

S-1: That's where I come in

S-1: I'm gonna be here and lucky for you, we live in the same state or our timezone is the same

[...]

S-1: I'm willing to talk to you often so you don't get lonley

S-1: I just need you to be sure if you want to do this or not

V-1: It's not the same as irl tho I have a few online friends too haha

S-1: Yeah but I get the feeling if I were to be your irl friend you'd probably wanna have sex

[...]

S-1: Yeah I get a strong feeling you try to get with me

S-1: And I mean sex isn't a bad thing but it's the amount of people you have sex with that is

V-1: I would think about it but I wouldn't do it if you didn't want to lol

[...]

S-1: I probably wouldn't turn it down but I wouldn't want you to keep increasing the count

[...]

S-1: For instance if you don't mind can I see what you look like ?

18. V-1 then sent a selfie-style picture of herself to S-1, at which point S-1 replied, "You're very attractive." S-1 and V-1 continued to communicate through Reddit. When S-1 and V-1 were discussing V-1's desire to leave her home and live on her own, S-1 said, "You can come stay with me haha," then said he was joking. At approximately 4:29 PM, S-1 told V-1, "Anyways you need to masturbate a lot more to get rid of your horniness," then asked V-1 how many times a day she masturbated.

19. On May 10, 2023, S-1 (still using the SUBJECT ACCOUNT) continued to communicate with V-1 through Reddit after V-1 told S-1 she was "horny." S-1 asked V-1 if she was trying to make him "sexually interested" in her. S-1 then asked V-1 if she wanted to have sex. When V-1 said she wanted to have "rough, humiliating, dehumanizing, degrading" sex, S-1 replied, "Only if

I don't have to use a condom," then told V-1, "And I intend to cum inside."

20. S-1 then asked V-1 if she had thongs and sweatpants and told V-1, "I want you to dress like this," before sending V-1 a picture of a female dressed in sweatpants and a small shirt. When V-1 sent pictures of the sweatpants she had, S-1 told V-1 to send them both, then said, "Show me the thongs."

21. S-1 and V-1 did not exchange additional messages until June 14, 2023, when S-1 and V-1 exchanged a small number of messages. After June 14, 2023, S-1 and V-1 (using Victim Account 1) did not exchange additional messages.

REDDIT CHATS BETWEEN SUBJECT ACCOUNT AND VICTIM ACCOUNT 2

22. On June 3, 2023, V-1 used Victim Account 2 to submit a post on Reddit regarding her desire to run away from her home. V-1 did not state her age in the post, but referenced needing to obtain a "fake ID."

23. On June 4, 2023, S-1 used the SUBJECT ACCOUNT to message V-1 on Victim Account 2, asking in his initial message, "Need help?" Based on the messages between S-1 and V-1 on Victim Account 2, S-1 did not realize he was communicating with the same person he had been messaging on Victim Account 1.

24. Early in the conversation, S-1 asked V-1 where she was from and how old she was. V-1 stated she was from Northern California, 15 years old, and almost 16 years old. S-1 told V-1 he was from Southern California and stated he was willing to "help" V-1 if she promised him to "get off drugs." S-1 then clarified, "And I mean hard drugs weed is ok."

25. S-1 asked V-1 if she was sure she wanted to run away and whether she is a "boy or girl." After V-1 answered those questions, S-1 replied, "Running is pretty hard and being a girl will only make it worse since many people are gonna ask you for sex in return for help." V-1 then told S-1 someone else had already told her they would trade a place to stay for sex. When S-1 asked if she was going to do that, V-1 said she was not going to. The conversations between S-1 (using the SUBJECT ACCOUNT) and V-1 (using Victim Account 2) ended on June 5, 2023.

IDENTIFICATION OF ABARCA

26. On August 14, 2023, in response to a United States Department of Homeland Security (DHS) summons, the PROVIDER sent me subscriber information associated with the SUBJECT ACCOUNT. The data indicated the SUBJECT ACCOUNT was created on December 5, 2022, and that it had an associated and verified email address of gilmarabarca3@gmail.com. The data also included multiple Charter Communications and T-Mobile Internet Protocol (IP) addresses associated with the activity of the SUBJECT ACCOUNT.

27. On August 22, 2023, in response to a DHS summons, Charter Communications produced data for three Charter Communications IP addresses that were associated with the SUBJECT ACCOUNT's activity on various dates and times. The subscriber for each IP address on each specific date and time was Maria Magana at the SUBJECT ADDRESS.

28. On August 25, 2023, in response to a DHS summons, T-Mobile produced subscriber information for two T-Mobile IP

addresses that were associated with the SUBJECT ACCOUNT's activity. Both IP addresses originated from a mobile device with phone number 714-860-5504.

29. On August 26, 2023, I searched the aforementioned phone number in a commercial database, which reported the phone number was associated with Gilmar ABARCA-Magana at the SUBJECT ADDRESS. I recognized the name from the email address associated with the SUBJECT ACCOUNT (gilmarabarca3@gmail.com). I subsequently learned through a government database that ABARCA was arrested in July 2022 in Orange County, California, for multiple state offenses related to illegal sexual activity with a minor.

30. On August 29, 2023, I reviewed the reports documenting the investigation into ABARCA from 2022. According to ABARCA's statement as documented in the reports, ABARCA had sexual intercourse multiple times with a 16-year-old female he originally met through Reddit. The reports also stated ABARCA purchased and provided a sex toy to the victim. Also, according to ABARCA's own statement as documented in the report, he took a picture of the victim's breasts and sent that picture to her through another social media application.

UNDERCOVER CHATS - VICTIM ACCOUNT 1

31. On August 24, 2023, while acting in an undercover capacity as V-1, I used Victim Account 1 to message the SUBJECT ACCOUNT, "Hey." Within five minutes of initiating the conversation, after some messages back and forth, S-1 asked, "Are you still fucking older men?" After I replied, "Took a

little break lol," S-1 asked, "Does that mean you'll be going back to it ?" Shortly after, S-1 asked, "Do I still ever get to smash?" When I asked S-1, "Are you going to come here?", S-1 replied, "If I did would I hit?" Based on my training and experience, I believe S-1 was using "smash" and "hit" as slang for sex.

32. I then told S-1 I was not previously honest about my age and told him I had just turned 14 years old. S-1 asked what age V-1 had previously claimed to be (16 years old) and what grade she was in. S-1 then said, "I guess it's fine. Do you wanna fuck me ?" I subsequently replied, "I mean I'm trying to be better lol. But maybe." Shortly later, S-1 said, "If that maybe ever turns into a yes let me know."

33. S-1 claimed, "I never got your pic." When I asked for clarification, S-1 replied, "Just of you," then said he would send a picture of himself if I sent a picture of myself and a picture he previously requested of V-1 in sweatpants and a thong. In response, I sent S-1 a picture of myself altered to look like a young female. S-1 replied, "Can you do the outfit one now :)). I was looking forward to it before you ghosted me." When I stated I could not yet send that picture, S-1 requested a picture of V-1 holding up three fingers, explaining, "I wanna verify you are who you are." Shortly after, I sent S-1 a picture of myself, altered to look like a young female, holding up three fingers. S-1 thanked me and stated, "I trust you now."

34. S-1 and I exchanged a small number of additional messages. When I asked why he had not yet sent a picture of

himself, S-1 replied, "Cause you didn't send the pic of the sweatpants like you promised." S-1 did not answer my response to that message.

UNDERCOVER CHATS - VICTIM ACCOUNT 2

35. On August 25, 2023, while acting as V-1, I used Victim Account 2 to message the SUBJECT ACCOUNT, "You disappeared." Shortly later, S-1 asked, "You still wanna run?" When I stated I did, S-1 asked, "Can I see you?" When I asked why, S-1 replied, "Cause I'm gonna help you? And if I help you irl I'd send up seeing you anyways." I then asked S-1 how he was going to help, to which he replied, "You tell me." When I replied, "Money. Or somewhere to stay," S-1 said, "Well if I helped with that then don't I at least deserve to see what you look like ?" I then sent S-1 a selfie-style picture of another HSI agent.

36. S-1 subsequently asked where I lived, when I wanted to leave, if others had offered help, and if I would have sex with the others if that was a condition of them helping me. When I responded I was not sure and asked S-1 if he was going to ask for "stuff," he replied, "If I did would you?" When I told S-1 "maybe" and asked him if he was asking, S-1 replied, "Would you do it? If I asked." S-1 and I ("UC") then exchanged the following messages:

UC: Is that what it's gonna take for you to help

S-1: Nah just wondering

S-1: I'll definitely sill help you

UC: Thank youu

UC: Probably too young for u anyway lol

S-1: So someone younger can smash but not me: (

UC: I mean I'm only 15 lol

UC: If you're into that [laughing-crying-face emoji]

S-1: So I can smash [one-eyebrow-raised emoji]

[...]

[August 26, 2023]

[...]

UC: How would I get there?

S-1: Uber, train, bus etc

UC: Train would probably be safest right?

S-1: Probably

UC: Would you pick me up from the train station there?

S-1: Of course

UC: Then what??

S-1: I don't know I can't take you in. In all honesty unless you have someone else to stay with I think it's best to bring you here, give you money and send you back

UC: Hmmm. Ok

UC: So just get round trip train tickets for the same day pretty much?

S-1: Yes

S-1: How much money would you want?

UC: I dunno

UC: \$500?? Lol

S-1: So can I fuck you too [thinking-face emoji]

UC: I thought you didn't wanna take me in lol

S-1: If I take you in I can smack?

S-1: Smash?

UC: Do you care if I'm a virgin??

S-1: Not really

UC: So you'll take me in and won't send me back if you can fuck me?

S-1: Would that be something you're ok with?

UC: I mean I'm pretty desperate to run and I would have no money or place to stay

S-1: So can I fuck you

UC: I guesss if that's what it'll take to get your help

S-1: So I can fuck you yes or no

UC: Will you take me in if I say no??

S-1: No I'd be too horny around you

UC: But you take me in if I fuck youu?

S-1: Yes

UC: Okk

UC: Yess you can

37. S-1 then said, "Let me see a pic of you." When I stated I had already sent one, S-1 said, "Yeah and I'm gonna need more. Imma verify you before I bring you here." Shortly after, S-1 stopped replying.

38. On August 28, 2023, I sent S-1 a message stating, "Heyyy are you gonna help me or not??" S-1 claimed he stopped responding because V-1 had not yet sent "the sweatpants pic." I determined S-1 was likely getting his conversations confused between Victim Account 1 (where he had requested "the sweatpants pic") and Victim Account 2. S-1 then requested I add him on Snapchat so he could obtain a verification picture and see my location through Snapchat. After some back and forth on Reddit, S-1 stopped responding to me.

PROBABLE CAUSE RELATED TO THE SUBJECT LOCATIONS

39. While ABARCA's California driver's license record reports a mailing address in Anaheim as of September 2020, there is probable cause to believe ABARCA currently resides at the SUBJECT RESIDENCE and regularly uses a 2018 Honda Civic (California license plate 8UNC499). This probable cause is based on the following facts:

a. ABARCA's California driver's license record shows that, in April 2022, law enforcement stopped ABARCA while he was driving the aforementioned Honda Civic. Registration records from the DMV report that the Honda is registered to Maria Luisa Magana at the SUBJECT RESIDENCE. Based on my investigation, I believe Maria Magana is ABARCA's mother.

b. In July 2022, local law enforcement spoke with ABARCA in front of the SUBJECT RESIDENCE after he arrived home from work. The interview was related to the investigation that led to ABARCA's 2022 arrest.

c. According to a commercial database, the address most recently associated with ABARCA is the SUBJECT RESIDENCE.

d. On September 7, 2023, at approximately 7:55 AM, an HSI agent observed ABARCA - who was driving the aforementioned Honda Civic - arrive at the SUBJECT RESIDENCE, park in its driveway, and enter the SUBJECT RESIDENCE.

REVIEW OF PROBABLE CAUSE

40. In conversations with V-1 on both accounts, S-1 did not hesitate to broach sexual topics. In chats with V-1 on Victim Account 1, despite V-1 telling S-1 she was 16 years old, S-1 asked V-1 multiple sexual questions and detailed how he would have sex with V-1. When I took over that specific conversation in an undercover capacity and told S-1 I was actually 14 years old instead of 16 years old, S-1 stated, "I guess it's fine," then asked, "Do you wanna fuck me ?"

41. In chats with V-1 on Victim Account 2, V-1 told S-1 she was 15 years old. When I took over that conversation in an undercover capacity, despite V-1 originally telling him her age and me reiterating it, S-1 eventually told me he would "take me in" as a runaway in exchange for sex.

42. Based on my training and experience, I know those who commit offenses such as the SUBJECT OFFENSE often do so over long periods of time and with multiple victims, either simultaneously or one after another. I have personally investigated cases where adult males were using the internet to

target multiple minor victims at the same time. Specific to this case, S-1 messaged V-1 on two separate Reddit accounts thinking two separate female children were using each account. V-1 told S-1 she was under 18 years old on both accounts, but each time, S-1 remained undeterred by V-1's age and continued inappropriate, sexual conversations with her and an undercover agent purporting to be her. Furthermore, based on my training and experience, I know those who commit the SUBJECT OFFENSE often solicit victims to take sexually explicit images and/or videos and send the images and/or videos to them.

43. Based on my training and experience, I believe it is probable S-1 is using the SUBJECT ACCOUNT to talk with minors other than V-1. S-1 used the SUBJECT ACCOUNT to initiate the chats with V-1 both times. If S-1 initiated chats with V-1 on two separate occasions and accounts, there is probable cause to believe S-1 has initiated conversations with other female children who have submitted posts to the same or similar subreddits. S-1's conduct as described in this affidavit shows he is seeking out Reddit users who appear vulnerable based on their public posts, as he only contacted V-1 - both in the case of Victim Account 1 and Victim Account 2 - after she posted in various subreddits seeking help and information related to problems she was experiencing in her personal life.

44. Furthermore, based on my training and experience, I am familiar with the tactics those who commit the SUBJECT OFFENSE use to groom their victims. For example, when S-1 was talking to V-1 on Victim Account 1, he claimed to care about her wellbeing,

explaining to her that he did not want her to kill herself and that he would not "do anything sexual" to her. However, as shown in this affidavit, S-1 quickly went back on his word with V-1. In a different example, when S-1 was chatting with V-1 on Victim Account 2, S-1 asked V-1 if she wanted help running away, then warned her that people would ask her for sex in exchange for helping her run away. S-1 subsequently did exactly that, telling me while I purported to be V-1 he would trade me shelter for sex.

45. Additionally, in the chats on both Victim Account 1 and Victim Account 2, S-1 broached the topic of "verifying" whether the person to whom he was talking was really a female child. Based on my training and experience, the more those who commit the SUBJECT OFFENSE do so, the more experienced they become in attempting to ensure they are not being scammed or targeted by law enforcement.

46. Based on information obtained from the PROVIDER and Internet service providers, there is probable cause to believe S-1 is ABARCA, a subject who was arrested for allegedly committing offenses related to the SUBJECT OFFENSE in 2022. The reports documenting ABARCA's 2022 arrest state he met that victim through Reddit. Therefore, I believe S-1 has been committing the SUBJECT OFFENSE using various Internet websites and applications, including Reddit, for some time and has targeted multiple victims in doing so.

47. Based on surveillance, multiple government and commercial databases, and OCSD's prior contact with ABARCA,

there is probable cause to believe ABARCA resides at the SUBJECT RESIDENCE and regularly uses the aforementioned Honda.

**VI. BACKGROUND REGARDING COMPUTERES,
CHILD EXPLOITATION, AND THE INTERNET**

48. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, knowledge, and conversations with other law enforcement personnel familiar with these types of investigations, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in sexually exploiting children interact with each other. Computers serve multiple functions in connection with child exploitation, including allowing people engaging in child exploitation to communicate and allowing for the production, distribution, and storage of child pornography. People engaged in seeking out children to exploit on the Internet will often store images of the exploited child in electronic format.

b. A computer's ability to store images in digital form makes the computer itself an ideal repository for images of child exploitation. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital

files. Large-capacity external and internal hard drives are common. Other media-storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, all which are very small devices that are plugged into a port on the computer. Additionally, it is extremely easy for an individual to take a photo or a video with a digital camera or smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to media-storage devices. Media-storage devices can easily be concealed and carried on an individual's person or in their vehicle. Mobile phones, including smart phones, can act as media-storage devices and are also often carried on an individual's person or in an individual's vehicle.

c. The Internet offers those involved in the sexual exploitation of children several different venues to meet and communicate as well to obtain, view, and trade child pornography, all in a relatively secure and anonymous fashion.

d. Individuals can use online resources (such as Yahoo! and Gmail, among others) to communicate regarding child exploitation and retrieve and store child pornography. These online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used,

however, evidence of the exploitation of minors using the Internet, such as child pornography, can be found on the user's computer or external media in most cases.

e. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files). Digital information can also be retained unintentionally. For example, traces of the path of an electronic communication may be automatically stored in many places. In addition to electronic communications, a computer user's Internet activities generally leave traces in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

49. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained

in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

50. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

51. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress ABARCA's thumb and/or fingers on the

device(s); and (2) hold the device(s) in front of ABARCA's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

52. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. BACKGROUND ON SOCIAL MEDIA

53. In my training and experience, I have learned that providers of social media services offer a variety of online services to the public. Companies like the PROVIDER allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with providers. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, phone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other email addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

54. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information

concerning subscribers and their use of the PROVIDER's services, such as account access information, email or message transaction information, and account application information. From my training and experience, I know such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

55. A subscriber of the PROVIDER can also store with the PROVIDER files other messages, such as address books, contact or buddy lists, calendar data, pictures or videos, notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

56. From my training and experience, I know social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service(s) utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, social media providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address

information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

57. From my training and experience, I know social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

58. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from

a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the email addresses or account identifiers and messages sent to that account, often provide important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of the SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with the SUBJECT ACCOUNT - without date restriction - for review by the search team.

59. Relatedly, the government must be allowed to determine whether other individuals had access to the SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

60. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime

involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B-II, is necessary to find all relevant evidence within the account.

61. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

62. As set forth in Attachment B-II, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

63. I make that request because I believe it might be impossible for a provider to authenticate information taken from the SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original

copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from the SUBJECT ACCOUNT.

64. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it - and its contents - may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government (e.g., if a defendant is incarcerated and does not or cannot access his or her account). Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

65. From my training and experience, I know the subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly; rather they use an algorithm (often referred to as a "hashing" algorithm) that is performed on the password and generates a new random of string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashing algorithm is performed

on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some providers insert additional text before or after the password, which is referred to as "salting" the password. The hashing algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively, or in addition to passwords, users may be required to select or propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user's password.

66. I know based on my training and experience that providers of social media services generally have access to and store the web or Internet browsing history of the user while he or she is logged into an account. That history can include the names and specific websites or URLs/URIs (Uniform Resource Locators or Indicators) of the sites that have been visited.

67. Providers of similar services will often keep track of what is referred to as "user agent string", which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include web requests; logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI, HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other email or social media accounts accessed by

or analytics related to the SUBJECT ACCOUNT. These can be used to determine the types of devices used while accessing the SUBJECT ACCOUNT, as well as data related to a user's activity while accessing the SUBJECT ACCOUNT.

68. I have also learned that providers of social media and email services often track the behavior and activities of persons using accounts by using cookies, which are strings of characters and numbers stored on a person's computer on their web browser. These cookies can often show whether more than one account was accessed by the same computer (and specifically the same web browser), as the provider can recognize that cookie when the same device returns to the service to access an account.

69. In order to identify other accounts used or maintained by the users of the SUBJECT ACCOUNT, the warrant also calls for the PROVIDER to disclose both (1) any cookies associated with the SUBJECT ACCOUNT (i.e., those cookies that were placed on any computers or web browsers) used to access the SUBJECT ACCOUNT, and (2) the identity of any other account(s) in which the same cookie or cookies used to access the SUBJECT ACCOUNT was/were recognized. If in the course of the investigation the digital devices used by the subject(s) of the investigation are found, they can be searched to determine if the cookies recognized by the provider are stored on those devices. The warrant also calls for the PROVIDER to identify any other accounts accessed by any computer or web browser using the same cookies as the SUBJECT ACCOUNT by providing subscriber records and log-in information

for those other accounts (but not to provide the contents of communications in those other accounts).

70. From my training and experience, I know users of accounts are often required to include an email account as well as a phone number in subscriber records. The email account may be an email account hosted at the same provider, or an account at a different provider. The email account is referred to by a number of names, such as a secondary email account, a recovery email account, or an alternative email account or communication channel. That email account is often used when the identity of the user of the primary account (here, the SUBJECT ACCOUNT) needs to be verified (e.g., if a password is forgotten) so the provider can confirm the person trying to access the account is an authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text (or "SMS") that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as "two-factor authentication" (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary email account and a secondary email account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary email account or to the phone number listed in subscriber records can allow access to the primary account.

71. From my training and experience, I know providers also keep a record of search queries run by the user of the account, whether searches within the services of the provider for persons, content, or other accounts (such as if a user is trying to find the account of an acquaintance), or broader Internet searches. In some instances, providers may also keep records of which websites or contents were "clicked on" as a result of these searches. This information is helpful in the context of the case to show the topics about which the user was trying to obtain more information or conduct research, and is relevant for "user attribution" evidence, analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

72. Providers also frequently obtain information about the types of devices that are used to access accounts like the SUBJECT ACCOUNT. Those devices can be laptop or desktop computers, cell phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the "hardware" or the physical device, some of which are assigned by a cell phone carrier to a particular account using cellular data or voice services, and some of which are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware models, operating system versions, unique device identifiers, Global Unique Identifiers ("GUIDs"),

serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control ("MAC") addresses, Electronic Serial Numbers ("ESNs"), Mobile Electronic Identity Numbers ("MEINs"), Mobile Equipment Identifiers ("MEIDs"), Mobile Identification Numbers ("MINs"), Subscriber Identity Modules ("SIMs"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDNs"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEIs"). Apple, one of the primary suppliers of mobile devices used to access accounts like the SUBJECT ACCOUNT, had previously used an identifier that was unique to the hardware of its devices, such that details of a device's activity obtained from a particular application could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID ("IDFA") that is still unique to a particular device, but which can be wiped and regenerated by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device's activity can be correlated across different applications or services. Google uses a similar advertiser ID referred to as an AAID.

73. These device identifiers can then be used to (a) identify accounts accessed at other providers by that same device, and (b) determine whether any physical devices found in the course of the investigation were the ones used to access the SUBJECT ACCOUNT. The requested warrant therefore asks for the

device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

74. Providers of social media and email often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in a number of ways. For example, a user may access the provider's services by running an application on the user's phone or mobile device. This application may have access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allow users to transmit or display their location to their "friends" or "acquaintances" via the provider.

IX. REQUEST FOR NON-DISCLOSURE

75. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscriber(s) of the SUBJECT ACCOUNT, of the existence of the warrants until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrants are signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in destruction of or tampering with evidence and/or otherwise seriously jeopardizing the investigation.

76. The federal investigation into ABARCA is not yet known by ABARCA or members of the public. Should ABARCA or others prematurely learn about the federal investigation, it is likely ABARCA and/or others will destroy or delete evidence.

X. CONCLUSION

77. Based on the foregoing, I request that the Court issue the requested warrants. The government will execute the warrant related to the SUBJECT ACCOUNT by serving the warrant on the PROVIDER. Because that warrant will be served on the PROVIDER, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the warrant at any time in the day or night. Investigators will execute the warrant related to the SUBJECT LOCATIONS during normal daytime hours.

Attested to by the applicant
in accordance with the
requirements of Fed. R. Crim.
P. 4.1 by telephone on this
_____ day of September 2023.

HONORABLE JOHN D. EARLY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-II

PROPERTY TO BE SEARCHED (REDDIT)

This warrant applies to information associated with Reddit account "Sweet-Explanation-81" (the "SUBJECT ACCOUNT") that is within the custody or control of Reddit Inc., a company headquartered at 548 Market Street, San Francisco, CA 94104, regardless of where such information is stored, held, or maintained.

ATTACHMENT B-II

ITEMS TO BE SEIZED (REDDIT)

I. SEARCH PROCEDURES

1. The warrant will be presented to personnel of Reddit Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images

of child pornography. The review of the electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A-II is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A-II:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, including:

i. All photographs, images, recordings, emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each

photograph, image, recording, email or message, and any related documents or attachments.

ii. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including

the dates on which such changes occurred, for the SUBJECT ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dialups, and locations.

iii. Any other account associated with the SUBJECT ACCOUNT including by means of sharing a common device, secondary, recovery, or alternate email address listed in subscriber records for the account, or phone number or SMS number listed in subscriber records for the account.

iv. Any information showing the location of the user of the SUBJECT ACCOUNT, including while sending or receiving a message using the SUBJECT ACCOUNT or accessing or logged into the SUBJECT ACCOUNT.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment AII, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2422(b), enticement of a child to engage in criminal sexual activity, namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Information related to how and when the SUBJECT ACCOUNT was accessed or used.

iii. Information, records, messages, communications, audio recordings, pictures, video recordings, or still captured images relating to the account user's or users' communication with suspected minors and/or solitication of sexually explicit content from minors.

iv. Child sexual abuse material or child erotica.

v. Information, in any form, relating to or tending to identify victims of the SUBJECT OFFENSE including records about their whereabouts.

vi. Information, in any form, tending to evidence the age of any suspected victim of the SUBJECT OFFENSES.

b. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the provider shall disclose

responsive data by sending it to the following address via US Mail, or to the following email address:

Davis Mendelsohn
100 Lighthouse Avenue, Monterey, CA 93940
415-271-6242 (cell); 831-647-7318 (fax)
davis.mendelsohn@ice.dhs.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

14. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-II, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 12 above of its intent to so notify.